ABSTRACT

A system and method for security management comprising log archival and reporting is provided using a novel architecture with particular application which is scalable for larger scale global data networks. The system comprises a Log Collection unit, interfacing with a Data Analysis and Log Archival unit, and a Data and System Access Unit interfacing with the Data Analysis and Log Archival Unit. The Log Collection Unit comprises a Log Collector Manager for managing log collection from a plurality log collectors interfacing with one or more security devices. The log collection unit transfers logfiles to a Storage Manager and a Data Analysis manager, connected to a Data Analysis Store, of the Data Analysis and Log Archival unit, which also comprises a Archival unit associated with the Storage unit.

The system provides for separation of logfile analysis and archival of logfiles, which improves scalability of the system. The Data and System Access unit provides a user interface for the system, preferably web based.